ApeosPort-IV 4070
ApeosPort-IV 3070
DocuCentre-IV 4070
DocuCentre-IV 3070

セキュリティ機能補足ガイド

ご注意
① 本書の内容の一部または全部を無断で複製・転載・改編することはおやめください。
② 本書の内容に関しては将来予告なしに変更することがあります。
③ 本書に、ご不明な点、誤り、記載もれ、乱丁、落丁などがありましたら弊社までご連絡ください。
④ 本書に記載されていない方法で機械を操作しないでください。思わぬ故障や事故の原因となることがあります。万一故障などが発生した場合は、責任を負いかねることがありますので、ご了承ください。
⑤ 本製品は、日本国内において使用することを目的に製造されています。諸外国では電源仕様などが異なるため使用できません。
また、安全法規制（電波規制や材料規制など）は国によってそれぞれ異なります。本製品および、関連消耗品をこれらの規制に違反して諸外国へ持ち込むと、罰則が科せられることがあります。

セキュリティ機能をお使いいただく前に

ここでは、認証されたセキュリティ機能に関する概要と確認事項を説明しています。

はじめに

本書は、本機を管理するシステム管理者を対象に、セキュリティ機能に関する設定手順と環境条件を説明しています。

また一般利用者を対象にセキュリティ機能に関する操作も補足しています。

他の機能の操作方法などについては下記のマニュアルをごらんください。

対象機種	マニュアル CD-ROM 帳票番号	PDF 帳票番号
ApeosPort-IV 4070/3070 DocuCentre-IV 4070/3070	電子マニュアル （HTML 形式） DE4758J1-1	ユーザーズガイド： ME5362J1-1
		管理者ガイド： ME5363J1-1

補足

- マニュアルの改訂により、帳票番号が変更になる場合があります。
- 電子マニュアル（HTML 形式）には、『ユーザーズガイド』『管理者ガイド』の内容がすべて含まれています。
- 『ユーザーズガイド』『管理者ガイド』の PDF ファイルは、マニュアル CD-ROM に格納されています。詳しくは、電子マニュアルの「注意制限・マニュアル一覧」をご覧ください。

富士ゼロックス　ApeosPort-IV 4070/3070、DocuCentre-IV 4070/3070 のセキュリティ機能は、以下の ROM バージョンで動作します。

Controller ROM Ver. 1.0.10

Controller ROM Ver. 1.40.10

ご注意
本製品は IT セキュリティ評価及び認証制度に基づき EAL3 を取得しています。
本製品が取得した情報セキュリティに係る認証は、評価に用いた評価対象（Target of Evaluation）が所定の評価基準及び評価方法に基づく評価の結果、セキュリティ保証要件に適合していることを示すものです。
尚、機械の改善や改良のため、Controller ROM バージョンが更新される場合があるため、お客様がお使いの機械の ROM およびマニュアルのバージョンが IT セキュリティ認証の対象バージョンとは異なることがあります。

セキュリティ機能

ApeosPort-IV 4070/3070、DocuCentre-IV 4070/3070 は、以下に示す認証されたセキュリティ機能を持ちます。

- ハードディスク蓄積データ上書き消去機能
- ハードディスク蓄積データ暗号化機能
- ユーザー認証機能
- システム管理者セキュリティ管理機能
- カストマーエンジニア操作制限機能
- セキュリティ監査ログ機能

- 内部ネットワークデータ保護機能
- ファクスフローセキュリティ機能

セキュリティ機能を有効にするための設定

セキュリティ機能を効果的に使用するために、システム管理者は以下の設定指示を遵守してください。

参照

・各設定の手順について詳しくは、以下の項で説明しています。
「セキュリティを有効にするための設定 1 （本機操作パネルからの初期設定）」(P.8)
「セキュリティを有効にするための設定 2（CentreWare Internet Services からの初期設定）」(P.14)
「セキュリティを有効にするための設定 3 （監査ログによる定期検査）」(P.19)

- パスワード使用 - パネル入力時
  ［する］に設定。
- 機械管理者パスワード
  工場出荷時の初期値を 9 文字以上の別のパスワードに変更。
- システム管理者の認証失敗アクセス拒否
  ［5］回に設定。
- カストマーエンジニアの操作制限
  ［する］に設定し、9 文字以上のパスワードを入力。
- ハードディスクの上書き消去
  ［1 回］あるいは［3 回］に設定。
- ハードディスクデータの暗号化
  ［する］に設定し、12 文字の暗号化キーを入力。
- 認証方式
  ［本体認証]、または［外部認証］に設定。
- アクセス制御
  ［デバイスへのアクセス］と［機能の使用制限］を［制限する］に設定。
  ［サービスへのアクセス］を［制限する（表示）]、または［制限する（非表示）］に設定。
- 認証 / プライベートプリント
  ［プライベートプリントに保存］に設定。
- パスワードの最小桁数
  ［9］桁に設定。
- スキャナー（URL 送信）
  無効に設定。
- ダイレクトファクス
  外部認証時は［禁止］に設定。
- ソフトウエアダウンロード
  ［禁止］に設定。
- 機械起動時のプログラム診断
  ［する］に設定。

- メール送信
  DocuCentre-IV では無効に設定。
- メール受信
  DocuCentre-IV では無効に設定。
- SMB
  NetBEUI を無効に設定。
- WebDAV
  外部認証時は無効に設定。
- LDAP サーバー
  LDAP サーバーの情報を設定。
- Kerberos サーバー
  Kerberos サーバーの情報を設定。
- IPP
  有効に設定。
- SSL/TLS 通信
  有効に設定。
- IPSec 通信
  有効に設定。
- SNMP v1/v2c
  無効に設定。
- SNMP v3
  有効に設定。
- S/MIME
  有効に設定。
- 監査ログ
  有効に設定。

注記

・各項目で上記以外の設定を行った場合は、セキュリティ機能を保つことができなくなりますので、ご注意ください。

・ファクスフローセキュリティ機能については、システム管理者による特別な設定は不要です。

・暗号化を無効にしてから、再度有効にする場合は、12 文字の暗号化キーを入力してください。

セキュリティ機能を最適に使用するために

本製品を利用・運用する組織の責任者は、次の事項を遵守してください。

- システム管理者、機械管理者の適切な人選を行うと共に、管理や教育を実施してください。
- 外部ネットワークから、本機を設置する内部ネットワークへのアクセスを遮断するために、ファイアウォールなどの機器を設置してください。
- パスワード（クライアント PC と本機のセットアップの両方に対して）と、暗号化キーは、次のルールに従って設定してください。
  - 容易に推測可能な文字列を使用しない
  - 英数文字を混在させて使用する

- システム管理者は、外部認証サーバーのアカウントポリシーを次のルールに従って設定してください。
  - パスワードポリシーを 9 文字以上に設定する
  - アカウントロックポリシーを 5 回に設定する
- ApeosWare Device Setup で本機と通信するときは、機械管理者 ID、パスワードを使用してください（機械管理の権限を与えられたユーザーはサポート外です）。
- 利用者はプリンタードライバーの［認証情報の設定］で、必ず User ID とパスワードを設定してください。
- 本機を管理するシステム管理者は、本機が対応する暗号化通信プロトコル（SSL/TLS、S/MIME、IPSec、SNMP v3）を、それぞれクライアント PC およびサーバー側のセキュリティ方針に沿って適用した上で、本機を運用してください。

■SSL/TLS

本機が接続する SSL クライアント（Web ブラウザー）および SSL サーバーには、以下の暗号化方式に対応したものを利用します。

（具体的には、Microsoft® 社の Internet Explorer® 6/7/8）

- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

■S/MIME

本機およびメールクライアントでは、以下の暗号化方式およびメッセージダイジェスト方式が利用されるように設定します。

- RC2/128 ビット、3Key Triple-DES/168 ビット、AES/128 ビット、AES/192 ビット、AES/256 ビット
- SHA1、SHA256

■PSec

本機が接続する IPSec ホストでは、以下の暗号化方式およびメッセージダイジェスト方式が利用されるように設定します。

- AES(128 ビット)/SHA1
- 3Key Triple-DES(168 ビット)/SHA1

■SNMP v3

SNMP v3 での共通鍵暗号方式は DES 固定です。メッセージダイジェスト方式は SHA1 を選択します。

ご注意
- 安全のために、CentreWare Internet Services を使用中は、他の Web サイトへアクセスしないでください。
- 安全のために、認証方式を変更する場合は、暗号化をリセットし暗号化キーを変更することで、ハードディスクを初期化してください。
- SSL の脆弱性を避けるために、ブラウザーのプロキシ例外リストに機械のアドレスを設定してください。機械とリモート PC 上のブラウザーが、プロキシサーバーを介さずに直接通信することで、中間者攻撃（MITM）を避けることができます。
- DocuCentre-IV は S/MIME 機能を有していないため、E メールとインターネットファクス機能は使用しないでください。

ROM バージョンとシステム時計の確認

初期設定を行う前に、システム管理者は機械の ROM バージョンとシステム時計が正しいことを確認してください。

操作パネルからの確認方法

1. 操作パネルの〈機械確認（メーター確認)〉ボタンを押します。
2. タッチパネルディスプレイの［機械状態 レポート出力］画面で、［ソフトウエアバージョン］を押します。

   画面上で、機械のソフトウエアバージョンを確認できます。

レポート出力による確認方法

1. 操作パネルの〈機械確認（メーター確認)〉ボタンを押します。
2. タッチパネルディスプレイの［機械状態 レポート出力］画面で、［レポート / リストの出力］を押します。
3. ［プリンター設定］を押します。
4. ［機能設定リスト（共通項目)］を押します。
5. 操作パネルの〈スタート〉ボタンを押します。

   プリントされたレポート上で、機械のソフトウエアバージョンを確認できます。

システム時計の確認方法

1. 操作パネルの〈認証〉ボタンを押します。
2. 〈数字〉ボタン、またはタッチパネルディスプレイに表示されるキーボードを使って、機械管理者 ID を入力します。
3. タッチパネルディスプレイの［確定］を押します。
4. ［仕様設定 / 登録］を押します。
5. ［仕様設定］を押します。
6. ［共通設定］を押します。
7. ［システム時計 / タイマー設定］を押します。

   画面上で時刻と日付を確認できます。設定変更が必要な場合は、以下の手順で変更してください。
8. 変更する項目を選択します。
9. ［確認 / 変更］を押します。

10 変更する項目を選択して、変更します。

11 ［決定］を押します。

12 ［閉じる］を２回押して、［仕様設定 / 登録］画面を終了します。

セキュリティを有効にするための設定１（本機操作パネルからの初期設定）

ここでは、セキュリティ機能に関連した初期設定について、本機の操作パネルで設定する手順について説明しています。

本機操作パネルからのパスワード使用の設定

1. 操作パネルの〈認証〉ボタンを押します。
2. 〈数字〉ボタン、またはタッチパネルディスプレイに表示されるキーボードを使って、機械管理者 ID を入力します。
3. タッチパネルディスプレイの［確定］を押します。
4. ［仕様設定 / 登録］を押します。
5. ［認証 / セキュリティ設定］を押します。
6. ［認証の設定］を押します。
7. ［パスワードの運用］を押します。
8. ［パスワードの運用］画面で、［パスワード使用 - パネル入力時］を押します。
9. ［確認 / 変更］を押します。
10. ［パスワード使用 - パネル入力時］画面で、［する］を選択します。
11. ［決定］を押します。
12. ［閉じる］を２回押して、［仕様設定 / 登録］画面を終了します。
13. 確認画面が表示されたら、［はい（再起動する）］を押します。

機械管理者モードに入るための認証

1. 操作パネルの〈認証〉ボタンを押します。
2. 〈数字〉ボタン、またはタッチパネルディスプレイに表示されるキーボードを使って、機械管理者 ID を入力します。
3. タッチパネルディスプレイの［次へ］を押します。
4. キーボードからパスワードを入力します。
5. ［確定］を押します。
6. ［仕様設定 / 登録］を押します。

機械管理者パスワードの変更

1 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。
2 ［機械管理者情報の設定］を押します。
3 ［機械管理者パスワード］を押します。
4 ［新しいパスワード］を押して、９文字以上のパスワードを入力します。
5 ［決定］を押します。
6 ［パスワードの再入力］を押して、パスワードを再入力します。
7 ［決定］を２回押します。
8 確認画面が表示されたら、［はい（変更する）］を押します。

システム管理者の認証失敗アクセス拒否回数の設定

1 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。
2 ［認証の設定］を押します。
3 ［機械管理ユーザーの認証失敗アクセス拒否］を押します。
4 ［機械管理権限ユーザーの認証失敗アクセス拒否］画面で、［する］を選択します。
5 ［▲］または［▼］を押して、[5］に設定します。
6 ［決定］を押します。

カストマーエンジニアの操作制限の設定

1 ［仕様設定 / 登録］画面で、［仕様設定］を押します。
2 ［共通設定］を押します。
3 ［その他の設定］を押します。
4 ［その他の設定］画面で、［カストマーエンジニアの操作制限］を押します。
5 ［確認 / 変更］を押します。
6 ［する］を押します。
7 ［保守パスワード］を押します。
8 ［新しいパスワード］を押して、９文字以上のパスワードを入力します。
9 ［決定］を押します。
10 ［パスワードの再入力］を押して、パスワードを再入力します。
11 ［決定］を押します。
12 ［閉じる］を押して、［決定］を押します。
13 確認画面が表示されたら、［はい（変更する）］を押します。
14 再度確認画面が表示されたら、［はい（変更する）］を押します。
15 ［閉じる］を押して、［その他の設定］画面を終了します。

ハードディスクの上書き消去の設定

1 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。

2 ［ハードディスクの上書き消去設定］を押します。

3 ［上書き回数の設定］を押します。

4 ［上書き回数の設定］画面で、［1 回］または［3 回］を押します。

5 ［決定］を押します。

ハードディスクデータの暗号化設定

1 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

2 ［共通設定］を押します。

3 ［その他の設定］を押します。

4 ［その他の設定］画面で、［データの暗号化］を選択します。

5 ［確認 / 変更］を押します。

6 ［する］を押します。

7 ［新しい暗号化キー］を押して、12 文字の暗号化キーを入力します。

8 ［決定］を押します。

9 ［暗号化キーの再入力］を押して、暗号化キーを再入力します。

10 ［決定］を２回押します。

11 確認画面が表示されたら、［はい（変更する)］を押します。

12 再度確認画面が表示されたら、［はい（再起動する)］を押します。

認証方式の設定

1 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。

2 ［認証の設定］を押します。

3 ［認証方式の設定］を押します。

4 ［認証方式の設定］画面で、［本体認証]、または［外部認証］を押します。

5 ［決定］を押します。

手順４で［外部認証］を選択した場合は、手順６以降を実行してください。

6 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

7 ［ネットワーク設定］を押します。

8 ［外部認証サーバー / ディレクトリサービス設定］を押します。

9 ［認証システムの設定］を押します。

10 ［認証システム］を選択します。

11 ［確認 / 変更］を押します。

12 ［認証システム］画面で、［LDAP］、［Kerberos（Windows2000）］、または［Kerberos（Solaris）］を選択します。

13 ［決定］を押します。

14 ［閉じる］を 2 回押して、［外部認証サーバー / ディレクトリサービス設定］画面を終了します。

アクセス制御の設定

1 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。

2 ［認証の設定］を押します。

3 ［アクセス制御］を押します。

4 ［デバイスへのアクセス］を押します。

5 ［デバイスへのアクセス］画面で、［制限する］を押します。

6 ［決定］を押します。

7 ［サービスへのアクセス］を押します。

8 ［サービスへのアクセス］画面で、機能を選択し［確認 / 変更］を押します。

9 ［制限する（表示）］、または［制限する（非表示）］を押します。

10 ［決定］を押します。

各機能に対し、手順 8 ～手順 10 の設定を行います。

11 ［閉じる］を押します。

12 ［機能の使用制限］を押します。

13 ［機能の使用制限］画面で、機能を選択し［確認 / 変更］を押します。

14 ［制限する］を押します。

15 ［決定］を押します。

各機能に対し、手順 13 ～手順 15 の設定を行います。

16 ［閉じる］を 2 回押して、［アクセス制御］画面を終了します。

プライベートプリントの設定

1 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。

2 ［認証の設定］を押します。

3 ［認証 / プライベートプリントの設定］を押します。

4 ［認証 / プライベートプリントの設定］画面で、［受信制御］を選択します。

5 ［確認 / 変更］を押します。

■本体認証を設定している場合

1) ［受信制御］画面で、［プリントの認証に従う］を選択します。

2) ［認証成功のジョブ］で［プライベートプリントに保存］を選択します。

3) ［認証が不正のジョブ］で［ジョブを中止］を選択します。

4) ［User ID なしのジョブ］で［ジョブを中止］を選択します。

■外部認証を設定している場合

1) ［受信制御］画面で、［プライベートプリントに保存］を選択します。

6 ［決定］を押します。

7 ［閉じる］を押して、［認証 / プライベートプリントの設定］画面を終了します。

パスワードの最小桁数の設定

注記

・本機能は、本体認証時のみ有効です。

1 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。

2 ［認証の設定］を押します。

3 ［パスワードの運用］を押します。

4 ［パスワードの運用］画面で、［パスワードの最小桁数］を選択します。

5 ［確認 / 変更］を押します。

6 ［パスワードの最小桁数］画面で、［指定する］を押します。

7 ［▲］または［▼］を押して［9］に設定します。

8 ［決定］を押します。

9 ［閉じる］を 2 回押して、［仕様設定 / 登録］画面を終了します。

10 確認画面が表示されたら、［はい（再起動する）］を押します。

スキャナー（URL 送信）の設定

1 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

2 ［共通設定］を押します。

3 ［画面 / ボタンの設定］を押します。

4 ［メニュー画面の機能配列］を選択します。

5 ［確認 / 変更］を押します。

6 ［スキャナー（URL 送信）］を押し［未設定］を選択します。

7 ［閉じる］を押します。

8 ［決定］を押します。

9 ［閉じる］を押して、［画面 / ボタンの設定］画面を終了します。

ダイレクトファクスの設定

外部認証を設定している場合は、次の設定を行い、ダイレクトファクス機能を［禁止］にしてください。

1. ［仕様設定 / 登録］画面で、［仕様設定］を押します。
2. ［ファクス設定］を押します。
3. ［ファクス動作制御］を押します。
4. ［ダイレクトファクスの使用］を押します。
5. ［確認 / 変更］を押します。
6. ［禁止］を選択します。
7. ［決定］を押します。
8. ［閉じる］を押して、［ファクス動作制御］画面を終了します。

ソフトウエアダウンロードの設定

1. ［仕様設定 / 登録］画面で、［仕様設定］を押します。
2. ［共通設定］を押します。
3. ［その他の設定］を押します。
4. ［その他の設定］画面で、［ソフトウエアダウンロード］を選択します。
5. ［確認 / 変更］を押します。
6. ［禁止］を押します。
7. ［決定］を押します。
8. ［閉じる］を押して、［その他の設定］画面を終了します。

機械起動時のプログラム診断の設定

1. ［仕様設定 / 登録］画面で、［仕様設定］を押します。
2. ［共通設定］を押します。
3. ［保守］を押します。
4. ［保守］画面で、［機械起動時のプログラム診断］を選択します。
5. ［する］を押します。
6. ［決定］を押します。
7. ［閉じる］を２回押して、［仕様設定 / 登録］画面を終了します。
8. 確認画面が表示されたら、［はい（再起動する）］を押します。

セキュリティを有効にするための設定 2 （CentreWare Internet Services からの初期設定）

ここでは、セキュリティ機能に関連した初期設定について、CentreWare Internet Services から設定する手順について説明しています。

CentreWare Internet Services からの設定準備

CentreWare Internet Services を利用するためには、ネットワークプロトコルとして TCP/IP が利用でき、「SSL/TLS」(P.5) の条件を満たす Web ブラウザーを有するコンピューターが必要です。

1. ご使用のコンピューター上で Web ブラウザーを起動して、アドレス入力欄に本機の TCP/IP アドレスを入力して、〈Enter〉キーを押します。
2. 認証を要求された場合は、機械管理者 ID とパスワードを入力します。
3. ［プロパティ］タブをクリックして、［プロパティ］画面を表示します。

メール送受信の設定

DocuCentre-IV の場合は次の設定を行い、メール送受信機能を無効にしてください。

1. ［プロパティ］画面で、［ネットワーク設定］をクリックします。
2. ［ポート起動］をクリックします。
3. ［メール送信］の［起動］チェックボックスのチェックを外します。
4. ［メール受信］の［起動］チェックボックスのチェックを外します。
5. ［新しい設定を適用］をクリックします。

SMB の設定

1. ［プロパティ］画面で、［ネットワーク設定］をクリックします。
2. ［ポート起動］をクリックします。
3. ［SMB］の［NetBEUI］チェックボックスのチェックを外します。
4. ［新しい設定を適用］をクリックします。

WebDAV の設定

外部認証を設定している場合は、次の設定を行い、WebDAV 機能を無効にしてください。

1. ［プロパティ］画面で、［ネットワーク設定］をクリックします。
2. ［ポート起動］をクリックします。
3. ［WebDAV］チェックボックスのチェックを外します。
4. ［新しい設定を適用］をクリックします。

LDAP サーバーの設定

1. ［プロパティ］画面で、［ネットワーク設定］をクリックします。
2. ［プロトコル設定］をクリックします。
3. ［LDAP］をクリックします。
4. ［LDAP サーバー / ディレクトリサービス］を選択します。
5. 各メニューから LDAP サーバーの情報を設定します。
6. ［新しい設定を適用］をクリックします。

Kerberos サーバーの設定

1. ［プロパティ］画面で、［セキュリティー］をクリックします。
2. ［外部認証サーバー設定］をクリックします。
3. ［Kerberos サーバー設定］を選択します。
4. 各メニューから Kerberos サーバーの情報を設定します。
5. ［新しい設定を適用］をクリックします。

注記

・Kerberos サーバーが外部認証サーバーとして設定されている場合、LDAP サーバーの［機械管理の権限］に、システム管理者権限を与えられたユーザーグループを設定することができます。

IPP の設定

1. ［プロパティ］画面で、［ネットワーク設定］をクリックします。
2. ［ポート起動］をクリックします。
3. ［IPP］チェックボックスをチェックします。
4. ［新しい設定を適用］をクリックします。

SSL/TSL の設定

1. ［プロパティ］画面で、［セキュリティー］をクリックします。
2. ［証明書の設定］をクリックします。
3. ［自己証明書の作成］をクリックします。
4. 必要に応じて、公開キーのサイズを設定します。
5. 必要に応じて、発行者を設定します。
6. ［新しい設定を適用］をクリックします。
7. ［SSL/TLS 設定］をクリックします。
8. ［HTTP － SSL/TLS 通信］、［LDAP-SSL/TLS 通信］の［有効］チェックボックスをチェックします。
9. ［新しい設定を適用］をクリックします。

10 ［再起動］をクリックします。

注記

- より安全な通信のために、［相手サーバーの証明書の検証］の［有効］チェックボックスをチェックし、「デバイス証明書のインポート」(P.16) と同じ手順で、サーバーの CA 証明書をインポートしてください。
- SMTP サーバーに SSL/TLS 機能がある場合、より安全な E-mail 通信のために、[SMTP- SSL /TLS 通信] を有効にしてください。

デバイス証明書のインポート

1 ［プロパティ］画面で、［セキュリティー］をクリックします。

2 ［証明書の設定］をクリックします。

3 ［証明書のインポート］をクリックします。

4 ［証明書］の欄にインポートするファイルの名前を入力します。または［参照］をクリックしてインポートするファイルを選択します。

5 ［パスワード］の欄にパスワードを入力して、［パスワードの確認］の欄に同じパスワードを入力します。

6 ［インポート］をクリックします。

IPSec の通信設定

注記

- ［IKE 認証方式］を［デジタル署名］に設定する場合は、設定する前に、「デバイス証明書のインポート」(P.16) と同じ手順で IPSec の証明書をインポートしておきます。

1 ［プロパティ］画面で、［セキュリティー］をクリックします。

2 ［IP Sec］をクリックします。

3 ［プロトコル］の［有効］チェックボックスをチェックします。

［IKE 認証方式］の欄で［事前共有鍵］を選択する場合は手順４～５、［デジタル署名］を選択する場合は手順６～ 11 の設定を行います。

4 ［IKE 認証方式］の欄で、［事前共有鍵］を選択します。これは本機と、クライアント PC およびサーバーとの通信を機密にするために使用します。

5 ［共有鍵］と［共有鍵の照合］の欄に共有鍵を入力します。
続けて、IPSec アドレスの設定を行います。

6 ［セキュリティー］の［証明書管理］をクリックします。

7 ［証明書の目的］の欄で、［IP Sec］を選択します。

8 ［一覧の表示］をクリックして、必要な証明書をチェックします。

9 ［証明書の表示］をクリックします。

10 ［証明書の選択］をクリックします。

11 ［IP Sec］画面の［IKE 認証方式］の欄で、［デジタル署名］を選択します。
続けて、IPSec アドレスの設定を行います。

IPSec アドレスの設定

1 ［IP Sec］画面で、［相手アドレスの指定［Ipv4］］の欄に、IP アドレスを入力します。

2 ［相手アドレスの指定［Ipv6］］の欄に、IP アドレスを入力します。

3 ［IPSec 未対応機器との通信］で、［通常の通信］または［通信しない］を選択します。

4 ［新しい設定を適用］をクリックします。

5 ［再起動］をクリックします。

SNMP v3 の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［プロトコル設定］をクリックします。

3 ［SNMP］をクリックします。

4 ［SNMP v3 を有効にする］チェックボックスをチェックします。

5 ［SNMP v1/v2c を有効にする］チェックボックスのチェックを外します。

6 ［新しい設定を適用］をクリックします。

7 ［SNMP］をクリックします。

8 ［SNMP v3 を編集する］をクリックして、［機械管理者によるアクセス］の［アクセスを許可する］チェックボックスをチェックします。

9 ［認証用パスワード（8 文字以上）］に新しい認証用パスワードを入力します。

10 ［パスワードの確認］に同じ認証用パスワードを入力します。

11 ［暗号化パスワード（8 文字以上）］に新しい暗号化パスワードを入力します。

12 ［パスワードの確認］に同じ暗号化パスワードを入力します。

13 ［プリントドライバーによるアクセス］の［アクセスを許可する］チェックボックスをチェックします。

14 ［新しい設定を適用］をクリックします。

注記

- 認証用パスワードと暗号化パスワードは必ず初期値から変更してください。
- SNMP v3 を使用する場合は IPSec プロトコルを同時に使用してください。そのために SNMP v3 クライアントの IP アドレスを「IPSec アドレスの設定」(P.17) の手順に従って設定してください。
- SNMP v1/v2 での通信はできませんので、プリンタードライバーのポートの設定は［SNMP ステータスを有効にする］のチェックを外してご使用ください。

S/MIME の設定

注記

- 本機のメール機能を使用するためには、『管理者ガイド』の「8 メール機能の設定」の手順でメール機能が有効になるように設定している必要があります。
- S/MIME を設定する前に、「デバイス証明書のインポート」(P.16) と同じ手順で、S/MIME の証明書をインポートしておきます。

1 ［プロパティ］画面で、［設定メニュー］をクリックします。

2 ［メール］の［設定］をクリックします。

3 ［メール設定］の［設定］をクリックして、［送信者アドレス］の欄に本機の E-mail アドレスを入力します。

4 ［新しい設定を適用］をクリックします。

5 ［セキュリティー］をクリックします。

6 ［証明書管理］をクリックします。

7 ［証明書の目的］の欄で、［S/MIME］を選択します。

8 ［一覧の表示］をクリックして、必要な証明書をチェックします。

9 ［証明書の表示］をクリックします。

10 ［証明書の選択］をクリックします。

11 ［SSL/TLS 設定］をクリックします。

12 ［S/MIME 通信］の［有効］チェックボックスをチェックします。

13 ［新しい設定を適用］をクリックします。

14 ［再起動］をクリックします。

15 本機が再起動したら、Web ブラウザーを更新（再読み込み）して、［プロパティ］タブをクリックします。

16 ［セキュリティー］をクリックします。

17 ［S/MIME 設定］をクリックします。

18 ［信頼できないメールの受信］チェックボックスのチェックを外します。

19 ［新しい設定を適用］をクリックします。

セキュリティを有効にするための設定 3 (監査ログによる定期検査)

ここでは、システム管理者のクライアント PC から CentreWare Internet Services を使用して、監査ログを設定し、取り出す手順について説明しています。

監査ログファイルは、セキュリティ管理者や外部の解析者の援助を得て定期的に検査することにより、試みられた機密漏洩に関し違反を識別して、また将来の違反を防止します。

監査ログ対象のイベント（例えば障害や構成変更、ユーザー操作など）は、タイムスタンプと共に NV メモリーに保存され、50 件単位で一つのファイル（以降、「監査ログファイル」と呼びます）として、最大 15,000 件まで本機のハードディスクへ保存されます。15,000 件を超えた場合は、一番古い監査ログイベントから順次消去され、繰り返してイベントが記録されます。監査ログの削除機能はありません。

監査ログの起動

1 Web ブラウザーを起動して、アドレス入力欄に本機の TCP/IP アドレスを入力して〈Enter〉キーを押します。
2 認証を要求された場合は、機械管理者 ID とパスワードを入力します。
3 ［プロパティ］タブをクリックします。
4 ［セキュリティー］をクリックします。
5 ［監査ログ］をクリックします。
6 ［監査ログの起動］の［有効］チェックボックスをチェックします。
7 ［新しい設定を適用］をクリックします。

監査ログファイルの取り出し

監査ログファイルの取り出し方法について説明します。

監査ログファイルへは、CentreWare Internet Services にシステム管理者として認証した場合だけアクセス可能で、操作パネルからアクセスすることはできません。

監査ログファイルをダウンロードする場合は、［HTTP-SSL/TLS 通信］が［有効］に設定されている必要があります。

1 Web ブラウザーを起動して、アドレス入力欄に本機の TCP/IP アドレスを入力して〈Enter〉キーを押します。
2 認証を要求された場合は、システム管理者の ID とパスワードを入力します。
3 ［プロパティ］タブをクリックします。
4 ［セキュリティー］をクリックします。
5 ［監査ログ］をクリックします。
6 ［監査ログの取り出し］の［txt ファイルで取り出す］をクリックします。

監査ログファイルには、次の情報が記録されています。アクセス、または試行の違反がないか、定期的にチェックしてください。

- Log ID：　監査ログ識別子としての通し番号
- Date、Time：　イベントが記録された日時
- Logged Events：　記録される事象の名称
- User Name：　事象を起こした利用者名
- Description：　イベントに関する内容の説明
- Status：　イベントの処理結果、または状態
- Optionally Logged Items：　共通保存項目以外に監査ログへ保存される追加情報

例：誰かが、User1 という ID でログインを試みて、パスワードの不一致のためにログインが失敗し場合、次の監査ログが記録されます。

Item	Description
Log ID	1
Date	01/01/2012
Time	10:00:00
Logged Events	Login/Logout
User Name	User1
Description	Login
Status	Failed (Invalid Password)
Optionally Logged Items	-

ユーザー認証

ここでは、本機を利用するためのユーザー認証の操作を説明しています。

本機を利用する前に、一般利用者は User ID とパスワードによる認証が必要です。

1 操作パネルの〈認証〉ボタンを押します。

2 〈数字〉ボタン、またはタッチパネルディスプレイに表示されるキーボードを使って、User ID を入力します。

3 ［次へ］を押します。

4 パスワードを入力します。

5 ［確定］を押します。

この状態で本機からの利用が可能になります。

注記

・他の人が使用している途中で割り込み操作を行う場合は、作業が終了したら必ず認証を解除してから割り込みを解除してください。

例：A さんの認証で使用中＞割り込み＞ B さんで認証（ログイン）＞割り込み作業
＞ B さんで認証解除（ログアウト）＞割り込み解除

補足

・外部認証を設定している場合、User ID とパスワードを入力する前に、［登録ユーザー］または［機械管理者］を選択してください。

・本体認証を利用する場合、機械管理者 ID だけが本機にあらかじめ登録されていますが、他の User ID は登録されていません。User ID の登録について詳しくは、『管理者ガイド』の「5 仕様設定」＞「認証 / セキュリティ設定」＞「認証の設定」＞「ユーザー登録 / 集計管理」を参照してください。

・外部認証を利用する場合、外部認証サーバーで管理されているユーザー情報を使用して認証するため、本機の機械管理者 ID は外部認証サーバーに登録されません。

付録

設定手順一覧

項目	操作パネルから	CentreWare Internet Services から	ApeosWare Device Setup から	初期値
日付、時刻の設定	［仕様設定］＞［共通設定］＞［システム時計 / タイマー設定］	ー	［設定］＞［機器の共通設定］＞［基本情報］＞［機器の時刻設定］	ー
本体パネルからのパスワード使用の設定	［認証 / セキュリティ設定］＞［認証の設定］＞［パスワードの運用］＞［パスワード使用 - パネル入力時］	ー	［設定］＞［機器の共通設定］＞［アクセス制限情報］＞［認証 / 集計情報］＞［認証 / 集計情報の設定］	無効
機械管理者パスワードの変更	［認証 / セキュリティ設定］＞［機械管理者情報の設定］＞［機械管理者パスワード］	［セキュリティー］＞［機械管理者情報の設定］	［設定］＞［機器の共通設定］＞［基本情報］＞［機械管理者情報の変更］	ー
システム管理者の認証失敗アクセス拒否回数の設定	［認証 / セキュリティ設定］＞［認証の設定］＞［機械管理ユーザーの認証失敗アクセス拒否］	［セキュリティー］＞［機械管理者情報の設定］	ー	5
カストマーエンジニアの操作制限の設定	［仕様設定］＞［共通設定］＞［その他の設定］＞［カストマーエンジニアの操作制限］	［セキュリティー］＞［カストマーエンジニアの操作制限］	ー	無効
ハードディスクの上書き消去の設定	［認証 / セキュリティ設定］＞［ハードディスクの上書き消去設定］	ー	ー	3 回
ハードディスクデータの暗号化設定	［仕様設定］＞［共通設定］＞［その他の設定］＞［データの暗号化］	ー	ー	無効
認証方式の設定	［認証 / セキュリティ設定］＞［認証の設定］＞［認証方式の設定］	［セキュリティー］＞［認証管理］	［設定］＞［機器の共通設定］＞［アクセス制限情報］＞［認証 / 集計情報］＞［認証 / 集計情報の設定］	無効
アクセス制御の設定	［認証 / セキュリティ設定］＞［認証の設定］＞［アクセス制御］	［セキュリティー］＞［認証管理］	ー	無効

項目	操作パネルから	CentreWare Internet Services から	ApeosWare Device Setup から	初期値
プライベートプリントの設定	[認証 / セキュリティ設定] ＞ [認証の設定] ＞ [認証 / プライベートプリントの設定]	ー	ー	無効
パスワードの最小文字数の設定	[認証 / セキュリティ設定] ＞ [認証の設定] ＞ [パスワードの運用] ＞ [パスワードの最小桁数]	[セキュリティー] ＞ [認証情報の設定] ＞ [パスワードの最小桁数]	ー	0
スキャナー（URL 送信）の設定	[仕様設定] ＞ [共通設定] ＞ [画面 / ボタンの設定] ＞ [メニュー画面の機能配列]	ー	ー	有効
ダイレクトファクスの設定	[仕様設定] ＞ [ファクス設定] ＞ [ファクス動作制御] ＞ [ダイレクトファクスの使用]	ー	ー	有効
ソウフトウエアダウンロードの設定	[仕様設定] ＞ [共通設定] ＞ [その他の設定] ＞ [ソフトウエアダウンロード]	ー	ー	有効
機械起動時のプログラム診断の設定	[仕様設定] ＞ [共通設定] ＞ [保守] ＞ [機械起動時のプログラム診断]	ー	ー	無効
メール送受信の設定	[仕様設定] ＞ [ネットワーク設定] ＞ [ポート設定]	[ネットワーク設定] ＞ [ポート起動]	[設定] ＞ [機器の共通設定] ＞ [基本情報] ＞ [ポート起動の設定]	無効
SMB の設定	ー	[ネットワーク設定] ＞ [ポート起動]	ー	有効
WebDAV の設定	[仕様設定] ＞ [ネットワーク設定] ＞ [ポート設定]	[ネットワーク設定] ＞ [ポート起動]	[設定] ＞ [機器の共通設定] ＞ [基本情報] ＞ [ポート起動の設定]	有効
LDAP Server の設定	[仕様設定] ＞ [ネットワーク設定] ＞ [外部認証サーバー / ディレクトリサービス設定] ＞ [LDAP サーバー / ディレクトリサービス設定]	[ネットワーク設定] ＞ [プロトコル設定] ＞ [LDAP] ＞ [LDAP サーバー / ディレクトリサービス]	ー	ー
Kerberos Server の設定	[仕様設定] ＞ [ネットワーク設定] ＞ [外部認証サーバー / ディレクトリサービス設定] ＞ [Kerberos サーバー設定]	[セキュリティー] ＞ [外部認証サーバー設定] ＞ [Kerberos サーバー設定]	ー	ー

項目	操作パネルから	CentreWare Internet Services から	ApeosWare Device Setup から	初期値
IPP の設定	［仕様設定］＞［ネットワーク設定］＞［ポート設定］	［ネットワーク設定］＞［ポート起動］	ー	無効
SSL/TSL の設定	［仕様設定］＞［ネットワーク設定］＞［セキュリティ設定］＞［SSL/TLS 設定］	［セキュリティー］＞［証明書の設定］＞［自己証明書の作成］＞［SSL/TLS 設定］	ー	無効
デバイス証明書のインポート	ー	［セキュリティー］＞［証明書の設定］＞［証明書のインポート］	ー	ー
IPSec の通信設定	［仕様設定］＞［ネットワーク設定］＞［セキュリティ設定］＞［IPSec 設定］	［セキュリティー］＞［IPSec］	ー	無効
SNMP v3 の設定	ー	［ネットワーク設定］＞［プロトコル設定］＞［SNMP］	ー	無効
S/MIME の設定	［仕様設定］＞［ネットワーク設定］＞［セキュリティ設定］＞［S/MIME 設定］	［セキュリティー］＞［SSL/TLS 設定］＞［S/MIME 通信］	ー	無効
監査ログの起動、取り出し	ー	［セキュリティー］＞［監査ログ］	ー	無効

ApeosPort-IV 4070/3070
DocuCentre-IV 4070/3070
セキュリティ機能補足ガイド

著作者 ― 富士ゼロックス株式会社　　発行年月 ― 2013 年 6 月　　第 1 版
発行者 ― 富士ゼロックス株式会社

（帳票番号 :ME6587J1-1）